**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEW JERSEY**

| | | |
|---|---|---|
| | : | **Mag. No. 16-4116** |
| **IN RE SEARCH WARRANT TO GOOGLE, INC.** | : | |
| | : | **OPINION** |

**HAMMER, U.S.M.J.**

This matter comes before the Court on the Government's motion to compel Google, Inc. ("Google") to comply with a search warrant directing Google to disclose records pertaining to electronic communications. Also before the Court is Google's application to quash the warrant to the extent it demands additional production. The Court has considered the papers submitted in support of, and in opposition to, the motions. The Court heard oral argument on the motions on June 15, 2017. For the reasons set forth herein, the Court will grant the Government's motion to compel and deny Google's motion to quash.

## I. Background

### A. Procedural History

On December 19, 2016, the Court issued a search warrant pursuant to §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) of the Stored Communications Act, 18 U.S.C. § 2701 et seq. ("SCA"), to Google for the production of the contents of particular Google e-mail accounts. The Government's application for the warrant established probable cause that targets in the United States were engaged in federal criminal activity in the United States, involving United States victims.

In response, Google produced only data that it confirmed was stored in the United States. That data included e-mails, header information, historical subscriber information that Google had

preserved, current subscriber information, and correspondence between Google and the account-holder. Declaration of Mikella M. Hurley in Support of Google Inc.'s Response to Motion To Compel (May 4, 2017) ("Hurley Decl.") ¶ 4 & Exh. B (Jan. 6, 2017, Letter from Google to Special Agent). Relying on the Second Circuit's decision in In the Matter of a Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) ("Microsoft"), reh'g denied, 855 F.3d 53 (2d Cir. 2017), Google declined to produce any data stored in Google servers located outside of the United States. See Hurley Decl., Exh. B ("[T]o the extent responsive emails currently in the accounts contained emails with attachments, Google has not produced the attachments to those emails because the attachment files were not confirmed to be stored in the United States. See Microsoft, 829 F.3d 197. Google has, however, separately produced a file for each account containing the headers and bodies of any responsive emails that contained attachments."). Therefore, Google did not produce e-mail content that it could not confirm was stored in the United States, including attachments to e-mails that Google produced. Id. Google supplemented its production on April 25, 2017, but again relied on Microsoft for the proposition that "the SCA does not authorize courts to issue and enforce against US-based service providers warrants for the seizure of information stored exclusively outside the United States[.]" Id. ¶ 5 & Exh. C (Apr. 25, 2017, Letter from Google to Special Agent).

On April 21, 2017, the Government moved to compel Google to produce responsive data in its possession, custody, or control, regardless of whether the data is stored on servers located in the United States or abroad. On May 5, 2017, Google filed opposition to the Government's motion, and cross-motions to quash the Government's subpoena and to amend the Amended

Non-Disclosure Order.[1] On May 26, 2017, the Government filed a reply brief on the motion to compel, and a separate brief in opposition to Google's cross-motion to amend the Amended Non-Disclosure Order. The Court held oral argument on June 15, 2017.

**B. Google's Storage and Retrieval Practices**

The facts underlying the Government's motion to compel are not in dispute. Google is a United States corporation that is headquartered in California. In addition to offering various on-line search capabilities and other services, Google is an e-mail service provider. Google stores its customers' data, including e-mail content, on servers located in the United States and abroad. The components of a particular e-mail, such as the header, content, and any attachments may be broken down into smaller pieces of information, sometimes known as "shards," and stored on multiple servers, each in a different country. Google states that "[s]ome user files may also be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time." Letter from Google Legal Investigations Support to Special Agent, Jan. 6, 2017, Hurley Decl. Exh. B. Individually, these shards are unintelligible; it is not until Google reassembles the relevant shards that they form an intelligible and useable piece of information, such as an e-mail or an attachment to an e-mail. In the Matter of the Search of Information Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc., 16-mj-757, --- F. Supp.3d ---, 2017 WL 2480752 (D.D.C. June 2, 2017); In re Search Warrant No. 16-190-M-01 to Google, --- F. Supp.3d ---, 2017 WL 471564, *13 (E.D. Pa. Feb. 3, 2017).

[1] The Court reserves decision on Google's motion challenging the Amended Non-Disclosure Order, and will hold additional oral argument. The parties will meet and confer with each other on the scheduling of that argument and shall notify the Court, on or before July 14, 2017, of a mutually convenient date and time for it. The Amended Non-Disclosure Order remains in full force and effect pending a ruling on Google's motion to amend.

Google's network may move data from server to server, and therefore from country to country, as often as once per day. It does so automatically, and to maximize network performance. See Letter from Google Legal Investigations Support to Special Agent, Jan. 6, 2017, Hurley Decl. Exh. B. It follows, then, that Google does not consult with the subscriber or account holder regarding where the data will be located. There also is no indication that Google notifies the subscriber or account holder either before or after moving his or her data. The subscriber or account holder has no role in designating where his or her e-mail content and related data will be stored, and no reasonable expectation that Google will store it in any particular location, or that the data will remain in that location for a particular period of time. Additionally, because the components of a single file may move from server to server, and therefore country to country, daily, "[i]t is possible, therefore, that the location of data responsive to a search warrant may change between the time the warrant is sought from the Court and when it is served on Google." In the Matter of the Search of Information Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc., 2017 WL 2480752; In re Search Warrant No. 16-190-M-01 to Google, 2017 WL 471564, *3.

When Google receives a search warrant from United States law enforcement personnel, Google's Legal Investigations Support ("LIS") queries Google's network for responsive data. All of Google's LIS personnel are located at the company's California headquarters, and conduct the search for responsive data there. See In re Search Warrant No. 16-960-M-01 to Google, 2017 WL 4711564, *4. Once LIS personnel locate the responsive data, they compile it, review it, redact any information that exceeds the scope of the warrant, and provide a copy of the responsive data to the government in the United States. See, e.g., Letter from Google Legal

Investigations Support to Special Agent, Jan. 6, 2017, Hurley Decl. Exh. B; Letter from Google Legal Investigations Support to Special Agent, Apr. 25, 2017, Hurley Decl. Exh. C.

**C. The Stored Communications Act**

The SCA was enacted as Title II of the Electronic Communications Privacy Act of 1986. The SCA "is directed to disclosure of communication information by providers of electronic communications[.]" In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records, 620 F.3d 304, 306 (3d Cir. 2010). "[T]he Stored Communications Act aims to prevent 'potential intrusions on individual privacy arising from illicit access to "stored communications in remote computing operations and large data banks that stored emails."'" In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 276 (3d Cir. 2016) (quoting In re Google, Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 145 (3d Cir. 2015) (quoting Garcia v. City of Laredo, Tex., 702 F.3d 788, 791 (5th Cir. 2012)), cert. denied sub nom., Gourley v. Google, Inc., 137 S. Ct. 36 (2016)).

The SCA "imposes general obligations of non-disclosure on service providers" and articulates the circumstances under which service providers may or must divulge specific information to customers or the government. The first three sections of the SCA are most relevant here. Section 2701 prohibits, and prescribes criminal penalties for, obtaining or altering electronic communications through unauthorized access of an electronic communication service ("ECS") facility. 18 U.S.C. § 2701. Section 2702 prohibits ECS and remote computing service ("RCS") providers from disclosing stored communications and related data except in certain circumstances. Id. § 2702.

Section 2703 is titled "Required disclosure of customer communications or records." 18 U.S.C. § 2703. Section 2703 dictates what information and records an ECS or RCS must

disclose to the government, and under what circumstances. See Microsoft, 829 F.3d at 207 ("Regarding governmental access in particular, § 2703 sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government."). See also In re Search Warrant No. 16-960-M-01 to Google, Inc., 2017 WL 471564, *3. As the court in In the Matter of the Search of Information Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc. noted, "the government can compel disclosure from a service provider using one of three ascending tiers of legal process that are demarcated by the showing the government must make in order to utilize them[.]" 2017 WL 2480752. For example, under § 2703(c)(2), the government can obtain basic subscriber information through an administrative or grand jury subpoena. Under § 2703(c)(1), the government can obtain additional subscriber and service records, including records of user activity and the e-mail and IP addresses with which the subscriber may have communicated, but excluding the contents of communications, through an order from a court of competent jurisdiction.[2] To obtain the order, often known as a "§ 2703(d) Order," the government must

[2] A "court of competent jurisdiction" consists of:

> (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that –
>
> (i) has jurisdiction over the offense being investigated;
> (ii) is in or for a district in which the provider of a wire of electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or
> (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or
>
> (B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants[.]

18 U.S.C. § 2711(3).

establish "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." Id. § 2703(d). Finally, and most relevant here, §§ 2703(a) and 2703(b)(1)(A) require the government in most instances to obtain a search warrant to obtain the content of stored electronic communications.

**D. Extraterritoriality**

The central legal issue in the Government's motion to compel, as it was in Microsoft, is whether a search warrant that was issued pursuant to the SCA, and which requires an e-mail service provider to produce data that is responsive to the search warrant but stored on computer servers outside of the United States, violates the presumption against extraterritorial application of United States law. See Microsoft, 829 F.3d at 201. Accordingly, it is useful to provide a brief overview of the law on extraterritoriality.

It is well established that absent a clear statement of Congressional intent to the contrary, federal statutes apply only within the territorial limits of the United States. Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010). In Morrison, the Supreme Court provided a framework to determine whether a particular statute applies extraterritorially. First, the court must consider whether the statute includes "'the affirmative intention of the Congress clearly expressed' to give a statute extraterritorial effect." Id. (quoting EEOC v. Arabian American Oil Co., 499 U.S. 244, 248 (1991)). The court must "ask this question whether the statute in question regulates conduct, affords relief, or merely confers jurisdiction." RJR Nabisco Inc. v.

---

Section 2703(c)(1) also provides other means by which the government can obtain this information, such as through a warrant, or with the subscriber's consent. 18 U.S.C. § 2703(c)(1)(A)-(D).

European Community, 136 S. Ct. 2090, 2101 (2016). "When a statute gives no clear indication of an extraterritorial application, it has none." Morrison, 561 U.S. at 255.

If there is no clear Congressional expression of extraterritorial application, the next step is to consider "whether the case involves a domestic application of the statute." RJR Nabisco Inc., 136 S. Ct. at 2101. The court must identify the focus of the statute, and then determine whether the conduct relevant to that focus occurs or would occur in the United States. Morrison, 561 U.S. at 265. If the conduct relevant to the statute's focus occurs in the United States, then there is no violation of the presumption against extraterritoriality, even if conduct outside the statute's focus occurs extraterritorially.

Applying this two-step framework, the Morrison Court concluded that § 10(b) of the Securities Exchange Act of 1934 did not embody a clear Congressional intent of extraterritorial application. Id. at 262-66. In the second step of the analysis, the Court rejected the argument that the complaint presented a permissible domestic application of § 10(b) because the alleged misrepresentations were made in the United States. The Court determined that § 10(b) focused on domestic securities transactions, not misrepresentations, and therefore did not provide a cause of action for sales of foreign securities, notwithstanding that the alleged misrepresentations culminating in the foreign transaction occurred in the United States. Id. at 268-69.

In RJR Nabisco Inc., the Court applied the Morrison framework in considering the extraterritoriality of particular sections of the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1961 et seq. The Court noted that RICO is unique because although Congress did not explicitly provide that § 1962(c) applies extraterritorially, a number of RICO predicate offenses set forth in § 1961 clearly apply extraterritorially. RJR Nabisco, Inc., 136 S. Ct. at 2103. In short, the predicate offenses available to establish a pattern of racketeering

activity include offenses with extraterritorial application, and offenses that have no extraterritorial application. RJR Nabisco Inc., 136 S. Ct. at 2101-03. Accordingly, the Court concluded that Congress, by incorporating those predicates with extraterritorial application into RICO, had provided a "clear, affirmative indication that § 1962 applies to foreign racketeering activity – but only to the extent that the predicates alleged in a particular case themselves apply extraterritorially." Id. at 2102. The Court concluded that "[a] violation of § 1962 may be based on a pattern of racketeering that includes predicate offenses committed abroad, provided that each of those offenses violates a predicate statute that is itself extraterritorial." Id. at 2103.

The Court also considered whether § 1964(c), which provides for a private right of action under RICO, allowed recovery for injuries sustained outside of the United States. The Court concluded that the statute itself provided no support for extraterritorial application. Id. at 2108.

**E. *Microsoft***

In Microsoft, the Second Circuit applied Morrison to invalidate a search warrant to the extent it sought to compel Microsoft to produce e-mail content from servers outside of the United States. In that case, the Government had obtained a search warrant under the SCA for the contents of a customer's e-mail account controlled by Microsoft. Microsoft produced the data stored in the United States, but moved to quash the warrant to the extent it sought anything outside of the United States, specifically information stored on servers in Dublin, Ireland. Unlike Google, Microsoft stored its customers' e-mail data "at datacenters located near the physical location identified by the user as its own when subscribing to the service[,]" in order to maximize network speed and efficiency. Microsoft, 829 F.3d at 202. When Microsoft designated a particular datacenter for a customer, it transferred all associated data for that

customer to that datacenter,[3] and deleted all substantive content from the servers in the United States. Id. at 203. Once Microsoft transferred the content to the designated data center and deleted it from the United States servers, that customer's e-mail content could be obtained only from the designated data center. Id. However, Microsoft personnel in the United States could access the data from the designated data center, which in that case was located in Dublin, Ireland.

The Magistrate Judge denied Microsoft's motion to quash. The court rejected Microsoft's argument that the warrant constituted an unauthorized extraterritorial application of United States law. The court recognized some ambiguity concerning the extent to which Federal Rule of Criminal Procedure 41[4] governed a warrant sought under the SCA. However, the

---

[3] Microsoft did not independently verify the user's location or identity before transferring the account information to the designated data center. "[I]t simply takes the user-provided information at face value, and its systems migrate the data according to the company protocol." Microsoft, 829 F.3d at 202.

[4] Federal Rule of Criminal Procedure 41 provides in pertinent part:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> . . . .
>
> (5) a magistrate judge having authority in the district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

Magistrate Judge determined that a warrant obtained under the SCA contained characteristics of both a search warrant and a subpoena:

> It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question.

In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp.3d 466, 471 (S.D.N.Y. 2014). Accordingly, the court rejected Microsoft's extraterritoriality argument, finding that the search would not take place until agents in the United States had reviewed the material. Id. at 472.

After the District Court affirmed the Magistrate Judge, Microsoft appealed to the Second Circuit. The Second Circuit reversed the District Court, finding that the warrant violated principles of extraterritoriality. The Second Circuit began its analysis by emphasizing the privacy protections afforded by the SCA. Id. at 206. The court noted that the SCA protects against unauthorized third parties accessing stored communications, and sets specific conditions for when the government may access information such as subscriber information, records of usage, and the content of stored communications.

The Second Circuit also noted that § 2703 of the SCA makes clear that warrants shall be issued "'using the procedures described in the Federal Rules of Criminal Procedure[,]'" and that Rule 41(b) restricts the "geographic reach of a warrant's execution[.]" Id. at 208 (quoting 18 U.S.C. § 2703). In light of those limitations, the Second Circuit considered whether the presumption against extraterritorial application of United States law, which "is strong and

---

(A) a United States territory, possession, or commonwealth . . . .

binding[,]" applied to warrants sought under § 2703. Id. at 209. Following the analytical framework set forth in Morrison, the Second Circuit first considered whether the SCA provides a clear indication that Congress intended it to apply beyond the United States sovereignty. The Second Circuit observed that the SCA lacks any "'affirmative indication'" of extraterritorial intent, unlike other statutes, such as 18 U.S.C. § 2331(1) and 18 U.S.C. § 2423(b), which contain such an expression. Id. at 211 (citing Weiss v. National Westminster Bank PLC, 768 F.3d 202, 207 & n.5 (2d Cir. 2014); United States v. Weingarten, 632 F.3d 60, 65 (2d Cir. 2011)).

The Second Circuit also rejected the lower courts' characterization of the SCA warrant as a hybrid warrant-subpoena. The Second Circuit concluded that characterization found no support in the statutory language of § 2703. Instead, the court reasoned, a private party who assists the government in conducting a search becomes an agent of the government, and is similarly bound by the Fourth Amendment's warrants clause. Id. at 214.

The Second Circuit also examined the SCA's use of "warrant," and concluded that it underscored the conclusion that Congress did not intend the SCA to have extraterritorial application. The Second Circuit reasoned that the purpose of a warrant is to limit the government's ability to invade the privacy of its citizens, such as by requiring the government to state with particularity the place to be searched and objects to be seized. Id. at 212. That limitation "is traditionally moored to privacy concepts applied within the territory of the United States." Id.

The Second Circuit next considered the second step of the Morrison analysis. The court found that the SCA focuses on maintaining the privacy of stored communications and not, as the government contended, on disclosure. Id. at 217-18. The court reasoned that the SCA establishes a sliding scale of protections for users by increasing the government's burden – from

subpoena, to § 2703(d) order, to search warrant -- according to the potential sensitivity of the data. Id. at 217. The court also considered the legislative history of the SCA, concluding its inclusion in the Electronic Communications Privacy Act "suggest[ed] privacy as a key concern." Id. The court also considered other sections of the SCA that are intended to protect the privacy of stored communications, such as § 2701, which prohibits unauthorized access of a stored electronic communication, and § 2702, which prohibits e-mail providers from knowingly disclosing stored electronic communications subject to specific exceptions. Id. at 218.

Having determined that the focus of the SCA is on privacy, the Second Circuit concluded that execution of the warrant would involve an impermissible extraterritorial application of the SCA. Id. at 220. The Second Circuit determined that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed – here, where it is seized by Microsoft, acting as an agent of the government." Id. The Second Circuit reasoned that the data would be seized from the Dublin data center, and therefore the conduct that is the focus of the SCA would occur there. Id. Therefore, the Second Circuit determined that "to enforce the Warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act." Id. at 221.

In a four-four decision, the Second Circuit denied rehearing en banc.[5] In the Matter of a Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation (Microsoft II), 855 F.3d 53 (2d Cir. 2017). The principle sources of disagreement between those judges who favored denying a rehearing en banc and those judges who favored

[5] Pursuant to Federal Rule of Appellate Procedure 35(a), a majority of active circuit judges must vote in favor of rehearing en banc.

granting it were: (1) the differences between a traditional Rule 41 search warrant and a warrant obtained under the SCA, and (2) whether privacy is the focus of the SCA for purposes of the second step of the Morrison analysis. Judge Raggi's dissent emphasized that

> a § 2703(a) warrant is not a traditional warrant. . . . It does not authorize federal agents to *search* any premises or to *seize* any person or materials. Rather, it authorizes a federal agent to require a service provider to disclose materials in its possession. The difference is significant to identifying where a warrant is being executed. Because a search warrant is executed with respect to a *place* – the place to be searched – the presumption against extraterritoriality expects that place to be within United States territory. By contrast, because a § 2703(a) warrant is executed with respect to a *person* – the person ordered to divulge materials in his possession – the presumption against extraterritoriality expects that person to be within United States territory and subject to the court's jurisdiction. If the person is so present, execution of the warrant as to him is a domestic application of United States law without regard to from where the person must retrieve the materials ordered disclosed.

Id. at 70 (citing Microsoft, 829 F.3d at 226 (Lynch, J., concurring in the judgment) (emphasis in original). That dissenting opinion also averred that the panel majority conflated privacy and sovereignty, and that United States search warrants have no extraterritorial effect because of the latter, not the former. Id. at 71. Judge Raggi further opined, "the panel errs in concluding that the privacy afforded by the SCA would be invaded by Microsoft's access of its own files in Dublin rather than by its subsequent disclosure of subscriber communications in the United States." Id. at 73.

In a separate dissent, Judge Cabranes reasoned that the "the activity that is the focus of the disclosure aspects of the SCA would necessarily occur in the United States where Microsoft is headquartered and where it would comply with the § 2703 warrant, not in the foreign country" where it stored the electronic communications. Id. at 75. Judge Cabranes also noted that Microsoft's decisions about where to store customers' electronic communications are not based on concerns for its customers' privacy, but on business considerations. Id. at 76.

Since Microsoft, a number of federal courts have considered this issue. Those courts have overwhelmingly concluded that requiring a domestic e-mail service provider to produce electronic communications stored on servers outside of the United States does not constitute an impermissible extraterritorial act. See In re Two Email Accounts at Google, Inc., Case No. 17-M-1235, 2017 U.S. Dist. LEXIS 101691 (E.D. Wis. June 30, 2017); In the Matter of the Search of Information Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc., Case No. 16-mj-757, --- F. Supp.3d ---, 2017 WL 2480752 (D.D.C. June 2, 2017); In the Matter of Search of Content that Is Stored at Premises Controlled by Google, Case No. 16-mc-80263-LB, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); In re Information Associated with One Yahoo Email Address that Is Stored at Premises Controlled by Yahoo, Case No. 17-M-1234, Case No. 17-M-1235, 2017 WL 706307 (E.D. Wisc. Feb. 21, 2017); In re Search Warrant No. 16-960-M-01 to Google, Misc. No. 16-960-M-01, --- F. Supp. 3d ---, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017). Indeed, the parties have not identified, nor has this Court found, any court decisions adopting or endorsing Microsoft.

## II. Discussion

### A. First Step of the *Morrison* Analysis

The first step in the extraterritoriality analysis requires the Court to determine whether the SCA contains an "'affirmative intention of the Congress clearly expressed' to give [the SCA] extraterritorial effect." Morrison, 561 U.S. at 255 (quoting Arabian American Oil Co., 499 U.S. at 248). On this issue, the Government offers two arguments. First, the Government argues that jurisdiction under § 2711(3) of the SCA contrasts with the typical in rem jurisdiction of Rule 41. See e.g., Fed. R. Crim. P. 41(b)(1) (providing that court "has authority to issue a warrant to search for and seize a person or property located within the district"). Memorandum of Law in

Support of Motion for an Order Directing Google To Comply with a Warrant for Disclosure of Records ("Govt. Moving Brief"), Apr. 21, 2017, at 7-8. The Government points to § 2711(3)(a)(i), which defines a "court of competent jurisdiction" to include a court "that . . . has jurisdiction over the offense being investigated[,]" and is not limited to the court wherein the object to be searched or seized is located. Once the court's jurisdiction is established, and upon an application by the government establishing probable cause, the provider is compelled to produce the items sought in the warrant. The Government reasons that "[b]y requiring disclosure to be made by a provider with control over the information sought, Congress eliminated the question of where that information may be stored." Govt. Moving Brief at 12. In this regard, the Government analogizes a district court's jurisdiction over a SCA warrant to enforcing its mandate over a private party in civil litigation—if the court has jurisdiction over the person or entity, it may compel that entity to produce any discovery in its custody or control, regardless of where that discovery is located. Id. at 10 & n.5 (citations omitted).

The Government's argument has some appeal. At least one court has relied on similar reasoning to find that a similar warrant to an e-mail service provider did not violate the presumption against extraterritoriality. See In re Information Associated with One Yahoo Email Address that Is Stored at Premises Controlled by Yahoo, 2017 WL 706307, *3. Moreover, it is true that the SCA expanded a court's authority to issue a warrant beyond Rule 41, by adding § 2711(3)(A)(i). With the addition of § 2711(3)(A)(i), a court's jurisdiction to issue a warrant is not premised solely on whether the information to be searched is located in that court's district, but also may derive from that court's jurisdiction over the offense under investigation. The Government also fairly avers that cloud-based data, unlike a desk or briefcase with documents inside it, may be accessed from any number of places. However, to the extent the Government

relies on in personam jurisdiction to satisfy the first step of Morrison, the argument fails for several reasons.

First, the Government's reasoning elides any consideration of the first step of Morrison. The Government contends that when Congress enacted the SCA and amended it in 2001, "[i]t did so with full knowledge of the consequences of structuring disclosures under the SCA" to eliminate consideration of the data's location. Id. at 12. But that argument falls well short of the expression of clear Congressional intent that Morrison instructs is necessary to rebut the presumption that United States law does not apply extraterritorially. Although Morrison requires such an expression of Congressional intent in any event, it would seem particularly necessary as to the SCA, because § 2703(a) requires the government to obtain a warrant "using the procedures described in the Federal Rules of Criminal Procedure" to compel the provider to disclose the content of communications that have been stored for 180 days or less. The Government's in personam jurisdiction argument is difficult to reconcile with the territorial limitations in Rule 41(b).

Second, as Google observes, even if the SCA established in personam jurisdiction, that would not necessarily suffuse the SCA with extraterritorial application. See Google, Inc.'s Response to Motion To Compel Compliance with Disclosure of Records, Motion To Quash, and Motion To Amend Nondisclosure Order ("Google Brief"), May 5, 2017, at 16. For example, an order authorizing a wiretap pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522, may direct the service provider to "furnish . . . all information, facilities, and technical assistance necessary to accomplish the interception[.]" However, federal courts have steadfastly held that Title III has no extraterritorial application. United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987); see also U.S. v. Londono-Cardona,

Crim. No. 05-10304-GAO, 2008 WL 313473, *2 (D. Mass. Feb. 1, 2008) (noting that "[c]ourts have repeatedly applied the general 'legal presumption' against extraterritorial application to Title III" and citing cases).

The Government next argues that the Council of Europe Convention on Cybercrime Treaty ("Cybercrime Convention") supplies the requisite evidence of Congressional intent to mandate providers to produce responsive information regardless of where it is stored. Govt. Moving Brief at 13. The Government contends that the Cybercrime Convention represents the commitment of the United States and approximately forty-nine other countries to treat "compelling a person or entity located domestically to produce data that is in its control or custody, regardless of location," as a "domestic exercise of power." Id. The Government observes that the Senate ratified the Cybercrime Convention in 2006, after enactment of the SCA. Id. Moreover, the State Department has interpreted relevant provisions of the Cybercrime Convention as allowing authorities "to order a person, including third party custodian of data, such as an ISP . . . to produce data, including subscriber information, that is in that person's possession or control." Id. at 13-14 (quoting Letter of Submittal from the Senate to the Department of State, attached as Exh. A to Govt. Moving Brief, at XV, Treaty Doc. 108-11).

The Government's reliance on the Cybercrime Convention to satisfy step one of Morrison is unavailing. The Government cites no legal authority for the proposition that a court can determine Congressional intent for a statute from Senate ratification of a treaty, much less that such an analysis satisfies the clear expression of Congressional intent that Morrison requires. See RJR Nabisco, Inc., 136 S. Ct. at 2100 ("Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application . . . . The question is not whether we think 'Congress would have wanted' a statute to apply to foreign conduct 'if it

had thought of the situation before the court,' but whether Congress has affirmatively and unmistakably instructed that the statute will do so.") (quoting Morrison, 561 U.S. at 261). Indeed, when the Senate ratified the Cybercrime Convention, it did so pursuant to its "Advice and Consent" function under Article II, Clause 2 of the Constitution. The Senate was not acting in its legislative capacity under Article I, § 1.

The Court concludes that a plain reading of the SCA reveals it does not contain a clear expression of Congressional intent of extraterritorial application. The SCA contains no such language, in sharp contrast to the RICO predicates that the RJR Nabisco Court determined could apply extraterritorially. See RJR Nabisco, Inc., 136 S. Ct. at 2101 (noting that: (a) § 1957(d)(2) applies to violations occurring outside the United States, if the defendant is a United States citizen; (b) §§ 351(i) and 1751(k) each expressly provides "'[t]here is extraterritorial jurisdiction over the conduct prohibited by this section[;]'" and (c) § 2332(a) "applies only to conduct occurring outside the United States" because it prohibits the murder of a United States national person, "'while such person is outside the United States[.]'" (emphasis in original) (citations omitted). See also Microsoft, 829 F.3d at 216; Microsoft II, 855 F.3d at 70 (Raggi, J., dissenting).

**B. Second Step of the *Morrison* Analysis**

The Court having determined that the SCA contains no clear expression of Congressional intent to rebut the presumption against extraterritoriality, the Court next must consider "whether the case involves a domestic application of the statute." RJR Nabisco Inc., 136 S. Ct. at 2101. To do so, the Court must first determine the focus of the SCA, and then determine whether the conduct relevant to that focus occurs or would occur in the United States. Morrison, 561 U.S. at 265. If the conduct relevant to the statute's focus occurs in the United States, then there is no

violation of the presumption against extraterritoriality, even if conduct outside the statute's focus occurs extraterritorially.

Even assuming the focus of the SCA is on privacy, this Court concludes that compelling Google to provide all responsive information to the search warrant issued in this matter, regardless of whether the information is stored on computer servers outside of the United States, does not violate the presumption against extraterritorial application of United States law. In short, the Court concludes that the warrant calls for a search and not a seizure, and that the conduct relevant to the extraterritorial analysis—i.e., the location of the search--occurs entirely in the United States.[6]

[6] Accordingly, the Court need not determine whether the focus of the SCA is on privacy or disclosure. But there is strong support for the proposition that the focus of the SCA generally, and § 2703 particularly, is on disclosure. To be sure, the SCA was enacted to protect users' privacy interests against unauthorized intrusions of stored communications and related data. In re Google, Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d at 145. But § 2703 accomplishes that protection by requiring the government to follow specific procedures, and make specific threshold showings, before disclosure can be compelled. See, e.g., 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider . . . of the contents of a wire or communication service, that is in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures prescribed in the Federal Rules of Criminal Procedure . . . ."). Sections 2703(b) and 2703(c) similarly permit the government to obtain disclosure of particular information upon a particular showing. See In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records, 620 F.3d at 306 ("Section 2703(a) covers the circumstances in which a governmental entity may require providers to disclose the contents of wire or electronic communications in storage; section 2703(b) covers the circumstances in which a governmental entity may require providers to disclose the contents of wire or electronic communications held by a remote computing service."). Accordingly, although the purpose of § 2703 is to protect privacy, the statute vindicates that interest by regulating disclosure.

In In the Matter of the Search of Information Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc., the court carefully examined § 2703 and concluded that "the most relevant conduct of those sections is not the provider's accessing customer data, but rather the disclosure of that data to law enforcement." 2017 WL 2480752 (emphasis in original). That court agreed with Judge Cabranes's dissent in Microsoft II: "Taken together, these provisions of the SCA are thus designed to 'protect [] user privacy by prohibiting unlawful access of customer communications . . . and by regulating a provider's disclosure of

It is well established that a search arises under the Fourth Amendment when "the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action."[7] Smith v. Maryland, 442 U.S. 735, 740 (1979). For a search to occur under the Fourth Amendment, there must be a subjective expectation of privacy in the object or location searched, and that subjective expectation must be objectively reasonable. U.S. v. Stanley, 753 F.3d 114, 118 (3d Cir. 2014) (quoting Free Speech Coalition, Inc., 677 F.3d at 543). "To be objectively reasonable, a defendant's expectation of privacy must be more than rational; society must be willing to recognize it as legitimate." Id.

A seizure of property "occurs when 'there is some meaningful interference with an individual's possessory interests in that property.'" Soldal v. Cook County, Ill., 506 U.S. 56, 62 (1992) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)). It is well settled that outright deprivation or destruction of the property is meaningful interference to constitute a Fourth Amendment seizure. See, e.g., Brown v. Muhlenberg Twp., 269 F.3d 205 (3d Cir. 2011) (holding that police shooting of family pet constituted seizure). In Soldal, for example, the Supreme Court concluded that the involvement of local law enforcement in removing a mobile

---

customer communication to third parties.'" Id. (quoting Microsoft II, 855 F.3d at 68 (Cabranes, J., dissenting)) (emphasis in Microsoft II). See also Microsoft II, 855 F.3d at 73 (Raggi, J., dissenting) ("I cannot agree with the panel that privacy is the focus of § 2703 and that subscriber privacy would be invaded in Ireland were Microsoft to access its subscriber files there. . . . But § 2703 identifies circumstances when the government nevertheless 'may require' service providers to disclose their subscribers' communications. This gives some force to the government's argument that the focus of § 2703 is compelled disclosure, not enhanced privacy.") (emphasis in original).

[7] A search also may occur "where the government unlawfully, physically occupies private property for the purpose of obtaining information." Free Speech Coalition, Inc. v. Attorney General of U.S., 677 F.3d 519, 543 (3d Cir. 2012). See also United States v. Jones, 565 U.S. 400, 404-05 (2012) ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

home to a nearby location, by removing the sewer and water connections and using a tractor for the removal, constituted a Fourth Amendment seizure.

However, merely copying a document or briefly examining an item does not necessarily amount to a Fourth Amendment seizure. In Arizona v. Hicks, the Supreme Court held that "the mere recording of the serial numbers [of stereo equipment in an apartment] did not constitute a seizure" because that act of recording, by itself, "did not 'meaningfully interfere' with respondent's possessory interest in either the serial numbers or the equipment[.]" 480 U.S. 321, 324 (1987). In United States v. Menon, a seafood importer whose offices were searched by Customs officers argued, inter alia, that the act of an agent taking documents from an assistant's desk for review by a supervising agent, during the search, constituted a seizure. 24 F.3d 550, 559-60 (1994). The Third Circuit dismissed the importer's seizure argument "with relative ease," finding that the agent's act of bringing the documents to the on-site supervising agent "did not 'meaningfully interfere with [his] possessory interest' in the documents to any extent greater than if [the agent] had brought [the supervising agent] to the documents." Id. at 560 (quoting Hicks, 480 U.S. at 324); see also Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992) (relying on Hicks to hold that "the recording of visual images of a scene by means of photography" by an officer lawfully on private property did not constitute a seizure because there was no meaningful interference with possession); United States v. Mastronardo, 987 F. Supp.2d 569, 576 (E.D. Pa. 2013) (relying on Hicks to hold that "[p]hotographing documents is not a seizure because it does not meaningfully interfere with a possessory interest in the documents").

This Court agrees with those courts that have held that "[e]lectronically transferring data from a server in a foreign country to Google's data center in California does not amount to a 'seizure' because there is no meaningful interference with the account holder's possessory

interest in the user data." In re Search Warrant No. 16-960-M-01 to Google, 2017 WL 471564, *9. See also In the Matter of the Search of Information Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc., 2017 WL 2480752 ("In fact, the service provider is not 'seizing' the data at all. . . . Merely copying a document or taking a photograph of material—both reasonable analogs to the instant case, where Google accesses and makes an electronic copy of a user's data—is not a 'seizure' of that material because there is no meaningful interference with the owner's possessory interest in it . . . ."). To comply with the warrant, Google does not remove the data from its server; it copies that data and provides the copy to the Government.[8] Not only is the account holder not deprived of the use of that data, the account holder is almost certainly unaware that Google has provided the data to the Government. In fact, the point of the Amended Nondisclosure Order that also is in dispute is the Government's effort to minimize the risk of notice to the account holder.

The issue then becomes the location of the search. The well entrenched definition of search—i.e., the existence of "a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action[,]" Smith, 442 U.S. at 740—compels the conclusion that the search occurs entirely in the United States. There is, quite simply, no invasion of privacy

[8] Google analogizes enforcement of the instant warrant to "the equivalent of requiring a hotel chain to search, seize, and retrieve to the United States luggage or correspondence a customer has stored in a room in a foreign hotel." Google Brief at 11. However, this characterization is readily dismissed. Requiring Google to query its servers for responsive data does not require any person to actually enter the foreign jurisdiction. And unlike the removed luggage, this warrant requires Google to copy the data rather than remove it. It will not deprive the account holder of the use of that data, and therefore does not constitute a seizure. See In the Matter of the Search of Information Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc., 2017 WL 2480752 ("Google's LIS representatives in California can access, compile, and disclose to the government those records and information with the push of a button and 'without ever leaving their desks in the United States.'") (quoting Microsoft, 829 F.3d at 229 (Lynch, J., concurring)).

in conjunction with execution of the instant warrant that will occur outside of the United States. First, and at the risk of stating the obvious, execution of the warrant will not entail a United States law enforcement officer leaving United States soil, much less conducting a physical inspection of a foreign location. Second, as explained above, the shards that Google will retrieve from its servers, whether in the United States or elsewhere, are, in their raw form, virtually useless to the Government. It is not until Google compiles and reassembles that data, at its California headquarters, and provides a copy of the responsive information to the Government, in the United States, that the Government can commence the search by examining the e-mails, attachments, and related data.

Google's own description of how it responds to receipt of a warrant buttresses this conclusion. According to Google, its process for responding to a warrant "includes determining where potentially responsive communications are stored; isolating the responsive communications from others stored in the same location; compiling the responsive communications; and sending them to Google personnel for production." Google Brief at 28. Google engages in each of those activities in the United States. The only event potentially occurring in a foreign jurisdiction is that the LIS personnel, in California, accesses that foreign server to copy (not remove) responsive data. Any contact with the foreign jurisdiction is perfunctory, particularly considering that Google might move that data to another server, in another country, the next day. Accordingly, the Court is satisfied that compelling Google to produce all material responsive to the warrant, even if that data is copied from foreign servers, does not run afoul of the presumption against extraterritorial application of United States law. See In re Search Warrant No. 16-960-01 to Google, 2017 WL 471564, *11 ("[T]he invasions of privacy will occur in the United States; the searches of the electronic data disclosed by Google

pursuant to the warrants will occur in the United States when the FBI reviews the copies of the requested data in Pennsylvania. These cases, therefore, involve a permissible domestic application of the SCA, even if other conduct (the electronic transfer of data) occurs abroad.").

## III. CONCLUSION

For the reasons set forth above, the Court concludes that the warrant at issue does not violate the presumption against extraterritorial application of United States law. Accordingly, the Court will grant the Government's motion to compel and deny Google's cross-motion to quash.

An appropriate form of Order accompanies this Opinion.

**Michael A. Hammer**
**UNITED STATES MAGISTRATE JUDGE**

Dated: July 10, 2017